Ubiquitous and Secure Networks and Services

Redes y Servicios Ubicuos y Seguros

Unit 2: Applications and Services

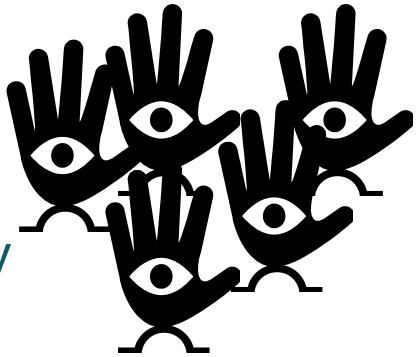
Ana Belén García Hernando
abgarcia@diatel.upm.es, anabelen.garcia@upm.es

Where does the great potential of ubiquitous systems come from?

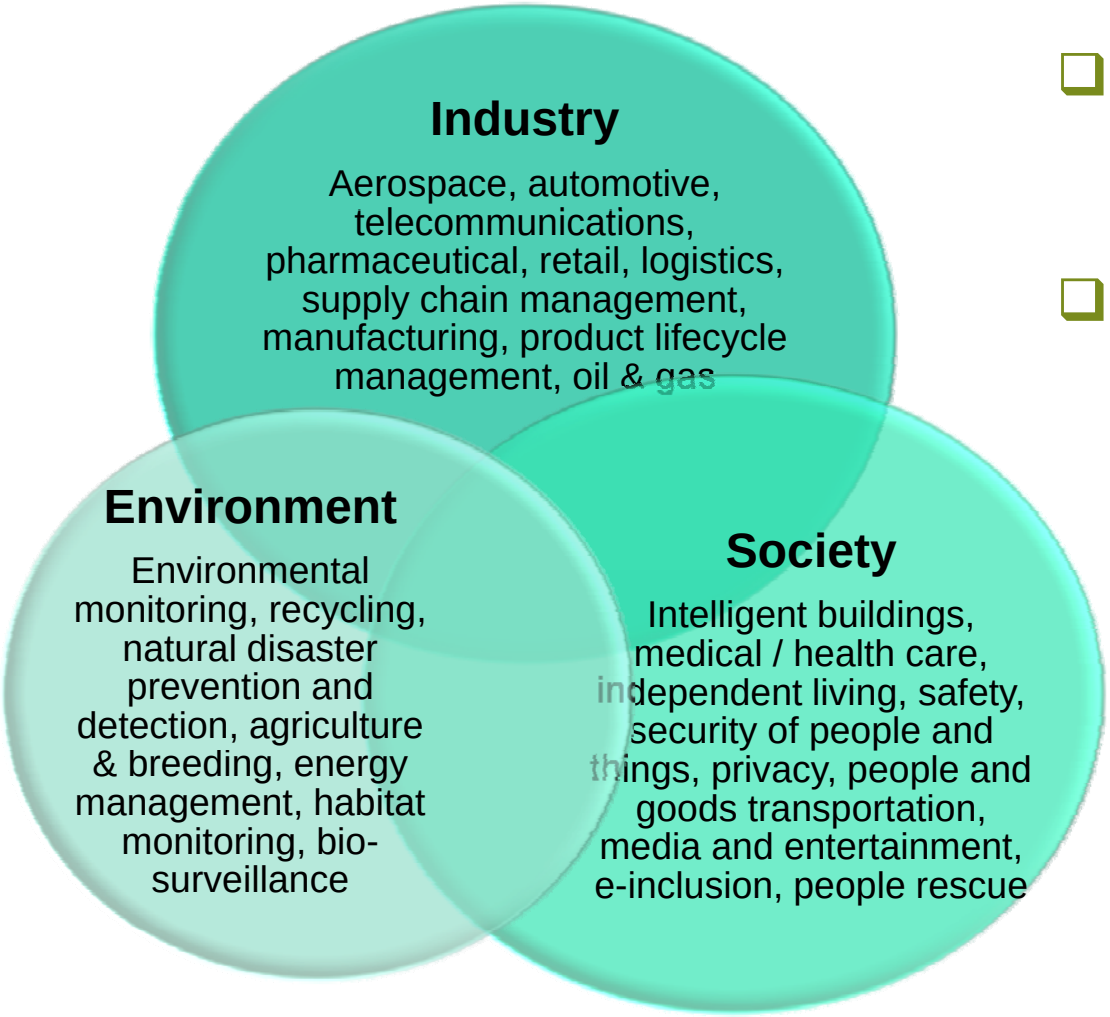
- Real time measurement and communication of physical phenomena, even in formerly inaccessible locations.
  - Huge amounts of information unveiled and available for its processing.
  - Enhanced response time (or prevention) of emergency situations.
  - Better quality of life, optimised industrial processes, safer cities and roads, more protected natural environments…

- Context awareness.

- Intelligence embedded in thousands (millions) of tiny nodes to offer services that are totally correlated with the reality (Ambient Intelligence).



Application domains

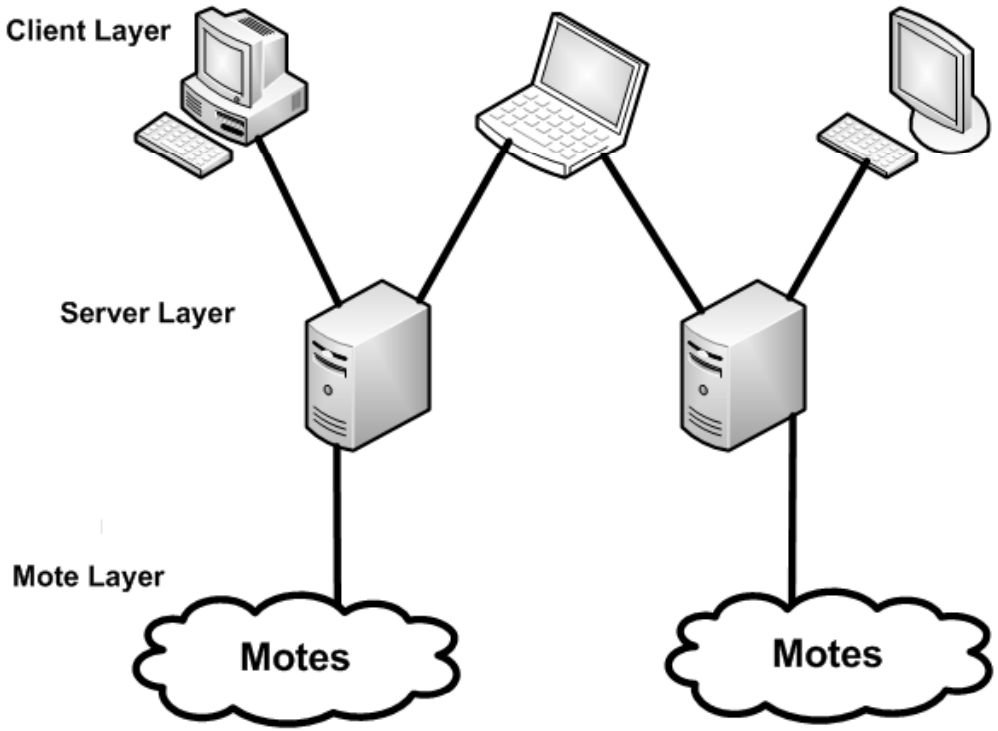


- This is just one of many possible classifications. The possible examples are countless.
- They are not isolated from one another: an application may contribute to more than one domain.

Applications and services

- Application: a whole system/ framework/ tool that supports one or more of the previous domains.
  - Applications and domains that are very different in purpose may pose quite similar requirements to services.
- The services cater for specific functionalities / needs of the intra / inter-domain level.
  - Target tracking, measurement of environmental parameters, query services, alarm generation.

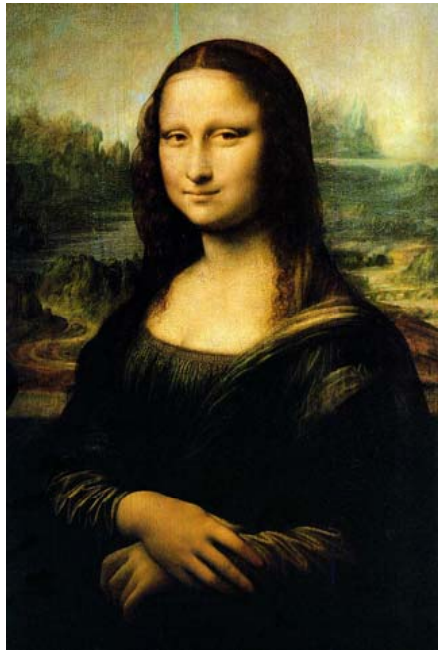
Simplified architecture of a WSN system



- The WSN itself may be accessed using services (abstractions) that imitate databases, web services, etc.
  - "intelligent middleware will allow the creation of a dynamic map of the real/physical world within the digital / virtual space" [CERP-IoT 2010]
- "In the long term, the borders between IoT and classic telecommunication networks will blur: a situation-aware service environment will be pervasively exploited (crossing different domains)." [CERP-IoT 2010]

Context awareness

"Little is more basic to human perception than physical juxtaposition, and so ubiquitous computers must know where they are. (Today's computers, in contrast, have no idea of their location and surroundings.) If a computer knows merely what room it is in, it can adapt its behavior in significant ways without requiring even a hint of artificial intelligence."
[Weiser 1991]



- Types of context:
  - User context: biometrics, attention, posture, …
  - Social context: surrounding people, type of group, link to other people, …
  - Environmental context: location, position, time, condition, energy, physical data, …

Factors facilitating / hindering a wide adoption of WSN / IoT applications

There is not a wide proliferation of commercial IoT products yet.	How to overcome this:
• Novel nonintrusive human-computer interaction model leads to an intrusive transition process for industries [Liu 2009] • Some public concerns, especially privacy and security. • Still a high number of standards. • The main domains for commercial use are home automation, building automation and medical. Smart energy and human mobility are emerging markets. [EETimes 2010]	• Leveraging existing infrastructures, devices, interfaces, development kits, … to overcome initial resistance. • More effort on standardization, harmonisation and socio-ethical issues. • The necessary reduction in costs and enhancement in battery lifetime and robustness.

Human – Computer Interface

"It [the computer] is approachable only through complex jargon that has nothing to do with the tasks for which people actually use computers. The state of the art is perhaps analogous to the period when scribes had to know as much about making ink or baking clay as they did about writing."
[Weiser 1991]

- Discuss in **class:** Is this still valid, 20 years after?

Human – Computer Interface

- The ideal case: a completely natural interaction

  "The hundreds of processors and displays are not a "user interface" like a mouse and windows, just a pleasant and effective "place" to get things done" [Weiser 1991]

- The reality: humans will still access applications and services using "conventional" HCI for some functions, although part of the interaction may be completely unnoticed.
  - GUIs, SMS, mobile calls, touch screens, voice interaction.
  - Interfaces for technical staff (e.g. a doctor, security personnel, …) should be different than those used by the general public.

Wireless parking scenario

Video:

Wireless Parking San Francisco

Location:

http://www.youtube.com/watch?v=yVq9pdam14M

- Do you find this application useful?
- Where is the intelligence of this system mainly located?

Wireless parking scenario

- Very basic sensors (detection of presence / absence of a car).
- The added value of this applications lies in the managing and interpretation of that distributed information.
  - Communication with the parking meter to start / renew a parking period.
  - Variable price depending on how congested the zone is.
  - Integration with other applications and services (restaurant reservation).
  - Even the mere compilation of information from the raw data (45% of parking sessions unpaid).
- Imagine upgrades to this application by
  - adding more intelligent nodes to cars, urban infrastructures, roads, … that measure parameters and communicate with each other:

  ITS (Intelligent Transport Systems), Smart cities, Smart roads

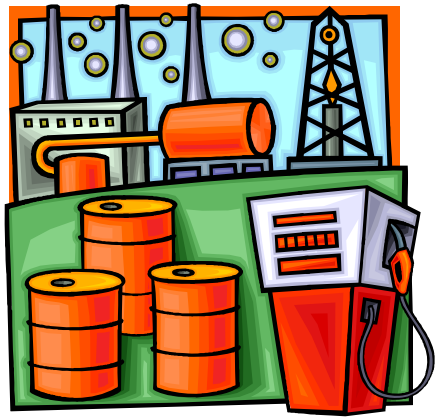
Quality of Service requirements

- QoS can be defined as the degree to which a system fulfils its requirements.
  - Not all applications have the same QoS requirements.
  - There is always a trade-off between QoS and consumption (this is especially important in WSN).
- QoS, in a broad sense, may be related to:
  - Network: delay, jitter (delay variation) and losses.
  - Sensing: measurement precision, spatial and temporal granularity, coverage.
  - Reliability: robustness, tamper-resistance, resilience.
  - Society and users: ease of use, privacy, anonymity, non-intrusiveness.

Privacy is one of the main concerns

- But aren't we sometimes willing to give it up?
- The "worrying" thing about IoT is that it could put privacy at risk without people even noticing.
- Security aspects of these systems have to be tackled from the beginning to gain users' confidence.

Oil drums scenario



Video:

Video about the CoBIs project broadcasted by SAP TV

Location:

http://www.cobis-online.de/files/SAP_At_Work_CoBIs_e_400kBit.wmv

- Are these sensing nodes more or less sophisticated than the previous ones?

Oil drums scenario

- Automation of industrial processes by embedding some degree of intelligence into things.
- Both managerial and security benefits.
- Some degree of decision-making in the WSN:
  - The WSN itself decides when an event needs further processing for sending it…
  - … in a distributed manner: sensors communicate with each other.
- Other possible applications: safety clothes.
- One of the main worries: Privacy. Why?
- Great reflection on business processes (less gap between the real time events and their reflection in the digital world).

Elderly care scenario

Video:

Video about the SODA project

Location:

See course materials.

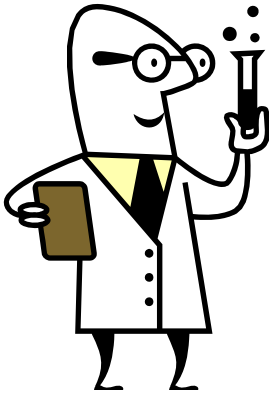
Video: Home Care, from the SODA project. Used with permission.

- What are the differences between the interfaces that are offered to:
  - The elderly person?
  - The relative of the elderly person?

Elderly care scenario

- Non-intrusiveness.
- Behavioural patterns recognition.
- Notification only if special conditions are detected.
  - Location of the person.
  - Communication with external services (e.g. sending video).
- Easy and known interfaces.
  - (Almost) not even noticed for the person at home.
  - Usual and known interfaces for family and friends receiving the warnings: sms, placing calls.

Some of the main technological challenges



- Hardware: Miniaturization, radio range, tamper resistance, batteries, …
- Network: Auto-configuration, network topologies, cross-layer optimization, QoS, routing, low duty cycle, synchronization, …
- Energy: Energy consumption (at all levels!), energy harvesting, …
- Software and applications: Low footprint, middleware, data abstraction, robustness, reutilization, usability, …
- Security: Confidentiality, privacy, authentication, …
- QoS (at several layers): possibility of coexistence of distinct applications, trade-off QoS-consumption, …

Bibliography

- [CERP-IoT 2010] Cluster of European Research Projects on the Internet of Things. Vision and Challenges for Realising the Internet of Things. March 2010.
- [CoBIs] “Collaborative Business Items” European project. http://www.cobis-online.de/
- [EETimes 2010] Mark LaPedus. Wireless sensor networks set to take off. April 2010. Online: http://www.eetimes.com/electronics-news/4088720/Wireless-sensor-networks-set-to-take-off
- [García 2008] García, A.B., Martínez, J.F. et al. Problem Solving for Wireless Sensor Networks. Springer-Verlag London Ltd., 2008.
- [IDTechEx 2010] IDTechEx. Active RFID and Sensor Networks 2011-2021. 2010.
- [Liu 2009] Yong Liu. Towards an open ubiquitous computing environment. IEEE International Conference on Pervasive Computing and Communications, 2009.
- [SFpark] SF park project. http://sfpark.org/
- [SODA] “Service Oriented Device & Delivery Architecture” European project. http://www.soda-itea.org/
- [Turon 2005] Turon, M. MOTE-VIEW: A Sensor Network Monitoring and Management Tool. The Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II), 2005.
- [Weiser 1991] Weiser, M. The computer for the 21st century. Scientific American, vol. 265(3), 1991.